PKYS.707

中华人民共和国国家知识产权局

邮政编码：100101 北京市朝阳区北辰东路 8 号汇宾大厦 A0601 北京市柳沈律师事务所 马莹,邵亚丽	发文日期 专利局 2005.10.21 发文
申请号:2004100019682	
申请人:三星电子株式会社	
发明创造名称:数据加密设备和方法	

中华人民共和国国家知识产权局 专利审查业务章

第一次审查意见通知书

1. ☑应申请人提出的实审请求，根据专利法第 35 条第 1 款的规定，国家知识产权局对上述发明专利申请进行实质审查。
   ☐根据专利法第 35 条第 2 款的规定，国家知识产权局决定自行对上述发明专利申请进行审查。
2. ☑申请人要求以其在：
   KR 专利局的申请日 2003 年 01 月 16 日为优先权日，
   专利局的申请日 年 月 日为优先权日，
   专利局的申请日 年 月 日为优先权日，
   专利局的申请日 年 月 日为优先权日，
   专利局的申请日 年 月 日为优先权日。
   ☐申请人已经提交了经原申请国受理机关证明的第一次提出的在先申请文件的副本。
   ☐申请人尚未提交经原申请国受理机关证明的第一次提出的在先申请文件的副本，根据专利法第 30 条的规定视为未提出优先权要求。
3. ☐经审查，申请人于：
   年 月 日提交的 不符合实施细则第 51 条的规定；
   年 月 日提交的 不符合专利法第 33 条的规定；
   年 月 日提交的
4. 审查针对的申请文件：
   ☑原始申请文件。 ☐审查是针对下述申请文件的
   申请日提交的原始申请文件的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的说明书摘要， 年 月 日提交的摘要附图。
5. ☐本通知书是在未进行检索的情况下作出的。
   ☑本通知书是在进行了检索的情况下作出的。
   ☑本通知书引用下述对比文献(其编号在今后的审查过程中继续沿用)：

编号	文件号或名称	公开日期（或抵触申请的申请日）
1	CN1304238A	2001.7.18

6. 审查的结论性意见：
   ☐关于说明书：
   ☐申请的内容属于专利法第 5 条规定的不授予专利权的范围。
   ☐说明书不符合专利法第 26 条第 3 款的规定。

回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收
（注：凡寄给审查员个人的信函不具有法律效力）

☐说明书不符合专利法第 33 条的规定。
☐说明书的撰写不符合实施细则第 18 条的规定。
☐_____

☑关于权利要求书：
☐权利要求_____不具备专利法第 22 条第 2 款规定的新颖性。
☑权利要求1-5, 7, 9, 11-17, 21-24, 26-31不具备专利法第 22 条第 3 款规定的创造性。
☐权利要求_____不具备专利法第 22 条第 4 款规定的实用性。
☑权利要求 35, 36 属于专利法第 25 条规定的不授予专利权的范围。
☐权利要求_____不符合专利法第 26 条第 4 款的规定。
☐权利要求_____不符合专利法第 31 条第 1 款的规定。
☐权利要求_____不符合专利法第 33 条的规定。
☐权利要求_____不符合专利法实施细则第 2 条第 1 款关于发明的定义。
☐权利要求_____不符合专利法实施细则第 13 条第 1 款的规定。
☑权利要求 7 不符合专利法实施细则第 20 条的规定。
☐权利要求_____不符合专利法实施细则第 21 条的规定。
☐权利要求_____不符合专利法实施细则第 22 条的规定。
☐权利要求_____不符合专利法实施细则第 23 条的规定。
☐_____

上述结论性意见的具体分析见本通知书的正文部分。

7. 基于上述结论性意见，审查员认为：
☐申请人应按照通知书正文部分提出的要求，对申请文件进行修改。
☑申请人应在意见陈述书中论述其专利申请可以被授予专利权的理由，并对通知书正文部分中指出的不符合规定之处进行修改，否则将不能授予专利权。
☐专利申请中没有可以被授予专利权的实质性内容，如果申请人没有陈述理由或者陈述理由不充分，其申请将被驳回。
☐_____

8. 申请人应注意下述事项：
(1)根据专利法第 37 条的规定，申请人应在收到本通知书之日起的肆个月内陈述意见，如果申请人无正当理由逾期不答复，其申请将被视为撤回。
(2)申请人对其申请的修改应符合专利法第 33 条的规定，修改文本应一式两份，其格式应符合审查指南的有关规定。
(3)申请人的意见陈述书和/或修改文本应邮寄或递交国家知识产权局专利局受理处，凡未邮寄或递交给受理处的文件不具备法律效力。
(4)未经预约，申请人和/或代理人不得前来国家知识产权局专利局与审查员举行会晤。

9. 本通知书正文部分共有 3 页，并附有下述附件：
☑引用的对比文件的复印件共 1 份 5 页。☐_____

审查员：刘[illegible](9848)
2005 年 9 月 30 日

审查部门 审查协作中心

回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收
（注：凡寄给审查员个人的信函不具有法律效力）

第一次审查意见通知书正文

1. 权利要求 35、36 属于专利法第二十五条第一款第二项规定的不授予专利权的范围。

权利要求 35、36 分别请求保护一种计算机可读记录介质，审查指南第二部分第九章第 2.1 节第六项指出：如申请的主题名称为一种存储计算机程序的计算机可读存储介质，但该计算机可读存储介质本身的物理特性没有发生任何变化，申请主题的实质是记录在该计算机可读存储介质上的计算机程序本身，由于计算机程序本身不给予专利保护，因此权利要求 35、36 属于专利法第二十五条第一款第二项规定的不授予专利权的范围。

2. 权利要求 7 不符合专利法实施细则第二十条第一款的规定。

权利要求 7 中涉及的“绝对差和信息”语义不清，因此导致权利要求的保护范围不清楚，不符合专利法实施细则第二十条第一款的规定。

即使申请人能够克服权利要求书的上述缺陷，权利要求书还存在以下缺陷。

3. 权利要求 1 至 5、7、9、11 至 17、21 至 24、26 至 31 不符合专利法第二十二条第三款的规定。

权利要求 1 请求保护一种加密设备，对比文件 1 公开了一种保密资料传送方法及系统，并具体公开了以下技术特征（参见其说明书第 6 页第 18 行至第 7 页第 9 行，附图 6、7）：在通讯端 5，特征抽取器 57 抽取输入资料的特征，并将其传送给装置 54，装置 54 根据接收到的信息生成通行码，单向函数装置 53 根据通行码生产加密密钥，编码解码器 56 根据该加密密钥对输入资料进行加密。本领域技术人员可以了解，对比文件 1 中的通行码等同于权利要求 1 中的随机数。权利要求 1 同对比文件 1 相比，其区别在于，1）在权利要求 1 中，处理的是音频/视频数据，而在对比文件 1 中，处理的是一般数据；2）在权利要求 1 中，预定数据是由内容处理器输出的；而在对比文件 1 中，特征信息是通过特征抽取器抽取的。对于区别技术特征 1），本领域技术人员可以了解，这是本领域技术人员常用的技术手段。对于区别技术特征 2），本领域技术人员可以了解，有关信息无论是通过内容处理器主动输出，还是通过特征抽取器抽取，这都是本领域技术人员常用的技术手段，都是能够提供和输入信息有关的信息。因此在对比文件 1 的基础上，结合本领域常用的技术手段以得到权利要求 1 所要求保护的技术方案，对本领域技术人员来说是显而易见的，因此权利要求 1 相对于对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二

十二条第三款有关创造性的规定。

权利要求 2、5、7、9、11、14 对权利要求 1 作进一步限定，权利要求 3 对权利要求 2 作进一步限定，权利要求 4 对权利要求 3 作进一步限定，权利要求 12、13 对权利要求 11 作进一步限定，权利要求 15 对权利要求 14 作进一步限定，其附加技术特征均为本领域技术人员常用的技术手段，因此当权利要求 1 相对于对比文件 1 不具备创造性时，对其作进一步限定的权利要求 2 至 5、7、9、11 至 15 相对于对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

权利要求 16 请求保护一种用于产生随机数的设备，对比文件 1 具体公开了以下技术特征（参见其说明书第 6 页第 18 行至第 7 页第 9 行，附图 6、7）：在通讯端 5，特征抽取器 57 抽取输入资料的特征，并将其传送给装置 54，装置 54 根据接收到的信息生成通行码。本领域技术人员可以了解，对比文件 1 中的通行码等同于权利要求 16 中的随机数。权利要求 16 同对比文件 1 相比，其区别在于，在权利要求 16 中，统计特定信息是由内容处理器输出的；而在对比文件 1 中，特征信息是通过特征抽取器抽取的。本领域技术人员可以了解，有关信息无论是通过内容处理器主动输出，还是通过特征抽取器抽取，这都是本领域技术人员常用的技术手段，都是能够提供和输入信息有关的信息。因此在对比文件 1 的基础上，结合本领域常用的技术手段以得到权利要求 16 所要求保护的技术方案，对本领域技术人员来说是显而易见的，因此权利要求 16 相对于对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

权利要求 17 对权利要求 16 作进一步限定，其附加技术特征均为本领域技术人员常用的技术手段，因此当权利要求 16 相对于对比文件 1 不具备创造性时，对其作进一步限定的权利要求 17 相对于对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

权利要求 21 请求保护一种加密方法，是与权利要求 1 相对应的方法权利要求，因此基于同评述权利要求 1 相类似的理由，权利要求 21 对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

权利要求 22、24、26、28 对权利要求 21 作进一步限定，权利要求 23 对权利要求 22 作进一步限定，权利要求 27 对权利要求 26 作进一步限定，权利要求 29 对权利要求 28 作进一步限定，其附加技术特征均为本领域技术人员常用的技术手段，因此当权利要求 21 相对于对比文件 1 不具备创造性时，对其作进一步限定的权利要求 22 至 24、26 至 29 相对于对比文件 1 不具有突出的实质性特

点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

权利要求 30 请求保护一种用于产生随机数的方法，是与权利要求 16 相对应的方法权利要求，因此基于同评述权利要求 16 相类似的理由，权利要求 30 相对于对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

权利要求 31 对权利要求 30 作进一步限定，其附加技术特征是本领域技术人员常用的技术手段，因此当权利要求 30 相对于对比文件 1 不具备创造性时，对其作进一步限定的权利要求 31 相对于对比文件 1 不具有突出的实质性特点和显著的进步，不符合专利法第二十二条第三款有关创造性的规定。

基于上述理由，申请人应根据上述审查意见在指定的期限内对申请文件进行修改，修改时应满足专利法第三十三条的规定，不得超出原说明书和权利要求书的记载范围。否则本申请将被驳回。申请人在答复一通时，必须针对一通中提出的问题进行修改，否则将可能导致申请文本不予接受。

The Patent office of the People's Republic Of China

Address: No. 6 XITUCHENG ROAD, JIMEN BRIDGE, HAIDIAN DISTRICT, BEIJING Post Code: 100088

Applicant:. SAMSUNG ELECTRONICS CO., LTD	ISSUING DATE: 2005. 10.21
Agent: Ye Li Shao	
Application No.: 200410001968.2	
Title: DATA ENCRYPTION APPARATUS AND METHOD	

THE FIRST OFFICE ACTION

1. ☑ The applicant filed a request for substantive examination on Year ____Month____Day____according to Article 35 Paragraph 1 of the Patent Law. The examiner has conducted a substantive examination to the above-mentioned patent application.

☐ According to Article 35 paragraph 2 of the Patent Law. Chinese Patent office decided on its own initiative to conduct a substantive examination to the above-mentioned patent application.

2. ☑ The applicant requested to take

Year 03 Month 01 Day 16 on which an application is filed with the KR patent office as the priority date.

Year_____Month_____Day_____on which an application is filed with the_____patent office as the priority date.

Year_____Month_____Day_____on which an application is filed with the_____patent office as the priority date.

☐ The applicant has submitted the copy of the earliest application document certified by the competent authority of that country.

☐ According to Article 30 of the Patent Law, if the applicant has not yet submitted the copy of the earliest application document certified by the competent authority of that country, the declaration for Priority shall be deemed not to have been made.

☐ This application is a PCT application.

3. ☐ The applicant submitted the amended document(s) on Year____Month____Day____and Year____Month_____Day after examination, _____submitted on Year_____Month_____Day_____is/are not accepted.

_____submitted on Year_____Month_____Day_____is/are not accepted

because the said amendment(s) ☐ is/are not in conformity with Article 33 of the Patent Law.

☐ is/are not in conformity with Rule 51 of the Implementing Regulations..

☐ The concrete reason(s) for not accepting the amendment(s) is/are presented on the text of Office Action.

4. ☑ The examination has been conducted based on the application text as originally filed.

☐ The examination has been conducted based on the following text(s):

page(s)_____of the specification, Claim(s)_____, and figure(s)_____in the original text of the application submitted on the filing day.

page(s)_____of the specification, claim(s)_____, and figure(s)_____submitted on Year____Month_____Day____

page(s)_____of the specification, claim(s)_____, and figure(s)_____submitted on Year____Month_____Day____

5. ☐ This notification was made without undergoing search.

☑ This notification was made with undergoing search.

☑ The following reference document(s) is/are cited:(the reference numeral(s) thereof will be used in the examination procedure hereafter)

NO.	Reference No. or Title	Publishing Date
1	CN1304238A	2001.7.18
2		
3		
4		
5		

6. Concluding comments

☐ on the specification:

- ☐ The contents of the application are in contrary to Article 5 of the Patent Law and therefore are not patentable.
- ☐ The contents of the application do not possess the practical applicability as prescribed in Paragraph 4 of Article 5 of the Patent Law.
- ☐ The specification is not in conformity with the provision of Paragraph 3 of Article 26 of the Patent Law.
- ☐ The presentation of the specification is not in conformity with the provision of Rule 18 of the Implementing Regulations.

☑ on the claims:

- ☐ Claim(s) _____ belong(s) to non-patentable subject matter as prescribed in Article 25 of the Patent law.
- ☐ Claim(s) _____ do(es) not comply with the definition of a patent as provided in Rule 2 paragraph 1 of the Implementing Regulations.
- ☐ Claim(s) _____ do(es) not possess novelty as requested by Article 22 paragraph 2 of the Patent Law.
- ☑ Claim(s) 1-5, 7, 9, 11-17, 21-26, 36-37 do(es) not possess inventiveness as requested by Article 22 paragraph 3 of the Patent Law.
- ☐ Claim(s) _____ do(es) not possess practical applicability as requested by Article 22 paragraph 4 of the Patent Law.
- ☐ Claim(s) _____ do(es) not comply with the provision of Article 26 paragraph 4 of the Patent Law.
- ☐ Claim(s) _____ do(es) not comply with the provision of Article 31 paragraph 1 of the Patent Law.
- ☑ Claim(s) 7 do(es) not comply with provision of Rule 20 of the Implementing Regulations.
- ☐ Claim(s) _____ do(es) not comply with provision of Rule 21 of the Implementing Regulations.
- ☐ Claim(s) _____ do(es) not comply with provision of Rule 22of the Implementing Regulations.
- ☐ Claim(s) _____ do(es) not comply with provision of Rule 23 of the Implementing Regulations.
- ☐ Claim(s) _____ do(es) not comply with the provision of Article 9 of the Patent Law.
- ☐ Claim(s) _____ do(es) not comply with the provision of Rule 13 paragraph 1 of the Implementing Regulations.

The detailed analysis for the above concluding comments is presented on the text of this Office Action.

7. Based on the above concluding comments, the examiner is of the opinion that

☐ The applicant should amend the application document(s) in accordance with the requirement as specified in the Office Action.

☑ The applicant should, in his observation, expound the patentability of the application of the application, amend the defects pointed out in the Office Action; or the application can hardly be approved.

☐ The examined deems that the application lacks substantive features to make it patentable. Therefore, the application will be rejected if no convincing reasons are provided to prove its patentability.

8. The applicant should pay attention to the following matters:

(1) According to Article 37 of the Patent Law, the applicant is required to submit his observations within **Four** months upon receipt of this Office Action. If the time limit for making response is not met without any justified reason, the application to have been withdraw.

(2) The amendment(s) made by the applicant must meet the requirements of Article 33 of the Patent Law. The amended text should be in duplicate, its format should conform to the related confinement in the Guidance for Examination.

(3) The applicant and/or the agent should not go to the Chinese Patent Office to interview the examiner without being invited.

(4) The observation and/of the amended document(s) must be mailed of delivered to the Receiving Section of the Chinese Patent Office. No legal effect shall apply for any document(s) that not mailed to or reached the Receiving Section.

9. The text of this Office Action contains 3 page(s), and has the following attachment(s):

☑ 1 copies of the cited references, all together 5 pages.

☐

Examination Dept. No._____ Examiner_____ Seal of Examination Dept. for business only _____

(if the Office Action wasn't stamped by the specified seal, it has no legal effect)

TEXT OF THE FIRST OFFICE ACTION

1. Claims 35 and 36 belong to the scope that no patent right shall be granted as prescribed in Article 25, clause 1, item 2 of the Chinese Patent Law.

Claims 35 and 36 seek protection for a computer-readable recording medium respectively. It is pointed out in Item 6, Section 2.1, Chapter 9, Part II of the Examination Guidelines: the title of the subject matter of an application for a patent for invention is a computer-readable storage medium for storing computer programs. However, there is no change in the physical feature of the computer-readable storage medium. The essence of the subject matter of the application is the computer program per se which is recorded in the computer-readable storage medium. Since no patent protection may be provided to the computer program per se, claims 35 and 36 belong to the scope no patent right shall be granted as prescribed in Article 25, clause 1, item 2 of the Chinese Patent Law.

2. Claim 7 does not comply with the provision of Rule 20, paragraph 1 of the Implementing Regulations of the Chinese Patent Law.

The "sum of absolute difference information" related in claim 7 is of unclear meaning. Consequently, claim 7 does not comply with the provision of Rule 20, paragraph 1 of the Implementing Regulations of the Chinese Patent Law in that its protection scope is not clear.

Even if the applicant can remove the above defects in the claims, the defects are still found in the claims as follows:

3. Claims 1 to 5, 7, 9, 11 to 17, 21 to 24, and 26 to 31 do not comply with the provision of Article 22, clause 3 of the Chinese Patent Law.

Claim 1 seeks protection for an encryption apparatus. Reference 1 has disclosed a method and system for transmitting secret data with detailed technical features as follows (refer to line 18 of page 6 to line 9 of page 7 in the specification, and Figs. 6 and 7): at the communication end 5, the feature extractor 57 extracts the features of the input material and transfers it to the device 54, the device 54 generates passing codes according to the received information, the one-direction function device 53 generates encryption key according to the passing codes, and the coding decoder 56 encrypts the input material according to said encryption key. Those skilled in the art can understand that the passing codes in Reference 1 are equivalent to the random number in claim 1. To compare claim 1 and Reference 1, the differences lie in: 1) it is audio/video data that is processed in claim 1, whereas common data is processed in Reference 1; and 2) it is the content processor that outputs the predetermined data in claim 1, whereas the feature information is extracted by the feature extractor in

Reference 1. As for the distinctive technical feature 1), those skilled in the art can understand it is an often-used technical measure for those skilled in the art. As for the distinctive technical feature 2), those skilled in the art can understand no matter the information is output initiatively by the content processor or is extracted by the feature extractor, they are both often-used technical measures for those skilled in the art, and they both can provide information relevant to the input information. Therefore, it is obvious for those skilled in the art to obtain the technical solution sought for protection in claim 1 by combining often-used technical measures in the art based on Reference 1. Consequently, claim 1 does not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law it that it does not possess any prominent substantive feature, nor does it represent a notable progress as compared with Reference 1.

Claims 2, 5, 7, 9, 11 and 14 make further definitions to claim 1, claim 3 makes a further definition to claim 2, claim 4 makes a further definition to claim 3, claims 12 and 13 make further definitions to claim 11, and claim 15 makes a further definition to claim 14. However, their additional technical features are all often-used technical measures for those skilled in the art. Therefore, when claim 1 does not possess inventiveness as compared with Reference 1, claims 2 to 5, 7, 9 and 11 to 15 do not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law in that they do not possess any prominent substantive feature, nor do they represent a notable progress as compared with Reference 1.

Claim 16 seeks protection for an apparatus for generating a random number. Reference 1 has disclosed the technical features as follows (refer to line 18 of page 6 to line 9 of page 7 in the specification, and Figs. 6 and 7): at the communication end 5, the feature extractor 57 extracts the features of the input material and transfers it to the device 54, and the device 54 generates passing codes according to the received information. Those skilled in the art, the passing codes in Reference 1 are equivalent to the random number in claim 16. To compare claim 16 and Reference 1, the difference lies in: it is the content processor that outputs statistical feature information in claim 16; whereas the feature information is extracted by the extractor in Reference 1. Those skilled in the art can understand: no matter the information is output initiatively by the content processor or is extracted by the feature extractor, they are both often-used technical measures for those skilled in the art, and they both can provide information relevant to the input information. Therefore, it is obvious for those skilled in the art to obtain the technical solution sought for protection in claim 16 by combining often-used technical measures in the art based on Reference 1. Consequently, claim 16 does not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law it that it does not possess any prominent substantive feature, nor does it represent a notable progress as compared with Reference 1.

Claim 17 makes a further definition to claim 16, and its additional technical feature is

an often-used technical measure for those skilled in the art. Therefore, when claim 16 does not possess inventiveness as compared with Reference 1, claim 17 making a further definition to claim 16 does not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law in that it does not possess any prominent substantive feature, nor does it represent a notable progress as compared with Reference 1.

Claim 21 seeks protection for an encryption method, which is a method claim corresponding to claim 1. Therefore, due to the reasons similar to those in the comments on claim 1, claim 21 does not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law in that it does not possess any prominent substantive feature, nor does it represent a notable progress as compared with Reference 1.

Claims 22, 24, 26 and 28 make further definitions to claim 21, claim 23 makes a further definition to claim 22, claim 27 makes a further definition to claim 26, and claim 29 makes a further definition to claim 28. However, their additional technical features are all often-used technical measures for those skilled in the art. Therefore, when claim 21 does not possess inventiveness as compared with Reference 1, claims 22 to 24 and 26-29 making further definitions to it do not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law in that they do not possess any prominent substantive feature, nor do they represent a notable progress as compared with Reference 1.

Claim 30 seeks protection for a method of generating a random number, which is a method claim corresponding to claim 16. Therefore, due to the reasons similar to those in the comments on claim 16, claim 30 does not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law in that it does not possess any prominent substantive feature, nor does it represent a notable progress as compared with Reference 1.

Claim 31 makes a further definition to claim 30, and its additional technical feature is an often-used technical measure for those skilled in the art. Therefore, when claim 30 does not possess inventiveness as compared with Reference 1, claim 31 making a further definition to it does not comply with the provision on inventiveness as prescribed in Article 22, clause 3 of the Chinese Patent Law in that it does not possess any prominent substantive feature, nor does it represent a notable progress as compared with Reference 1.

Due to the above reasons, the applicant should make amendments to the application document according to the above opinions within the specified time limit. It should be noted that the amendments should not go beyond the initial disclosure of the specification and claims so as to comply with the provision of Article 33 of the Chinese Patent Law. Otherwise, the present application will be rejected. When

making a response to the First Office Action, the applicant must make amendments in accordance with the problems brought forward in the First Office Action. Otherwise, it may render the application text unacceptable.

Examiner: Jianbo Liu

YYA

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 99126210.7

[43]公开日 2001年7月18日

[11]公开号 CN 1304238A

[22]申请日 1999.12.14 [21]申请号 99126210.7

[71]申请人 英属维京群岛盖内蒂克瓦耳有限公司
地址 英属维京群岛多尔拖拉路镇邮递区号34444
[72]发明人 后健慈

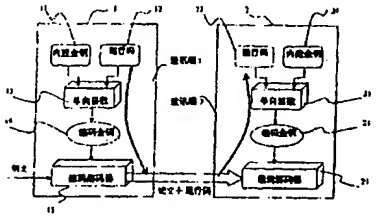
[74]专利代理机构 中国商标专利事务所
代理人 万学堂

权利要求书3页 说明书8页 附图页数11页

[54]发明名称 保护内建金钥及可变通行码的保密资料传送方法及系统

[57]摘要

本发明为一种保护内建金钥及可变通行码的保密资料传送方法及系统,一第一 内建金钥予该来源端,一第二内建金钥予该目的端;分配该机密资料为复数个 资料区块;产生复数个对于一资料区块的变化通行码;产生复数个工作金钥; 该工作金钥加密该资料区块;自该来源端传输该加密的资料区块及该变化的通 行码至该目的端;该目的端所接收的该变化通行码及该第二内建金钥来复原该工作 金钥;以及由该复原的工作金钥解密该加密资料区块。



ISSN1008-4274

步骤 S11：在来源端抽取如档案长度、属性、输入时间、定址等等特征；

步骤 S12：在来源端计算一基本通行码及抽取的特征的特定函数，以获得该真实通行码；

步骤 S13：在来源端利用该真实通行码及该内建金钥，以产生编码金钥，且藉由该编码金钥加密该相对应的资料区块；

步骤 S14：从该来源端将该资料区块连同该相对应的真实通行码传输至目的端；

步骤 15：在目的端利用所收到的通行码及其内的内建金钥以还原该编码金钥；

步骤 16：在目的端利用该区域产生的编码金钥以解密该接收的资料区块。

图 8 为实施例三的方块图。为简化起见，只有叙述该来源端 7。首先，资料被分段为几段区块 78，其是进一步分别输入至一 codec77 及一特征抽取器 74。于此同时，通行码 72 是由一随机变数产生器产生，其是同步于该资料段落 78。然后该通行码 72 及所抽取的特征是由一单向函数 73 所处理以产生真实通行码。与上述实施例一样，一内建金钥 71 及该真实通行码是由另外的单向函数 75 所处理以产生编码金钥 76，其是由该 codec77 所用，以加密该资料。如图 9 所示，在通讯端 8 中，由一函数 83 及一内建金钥 81 所产生的真实通行码是为一单向函数 85 所用，以产生编码金钥 86，其是进一步为一 codec87 所用，以解密该资料。同样，一与所接收的基本通行码合并的特征抽取器 84 是用以产生该真实通行码。本实施例结合实施例一及实施例二的基本原理。真实通行码是导自一该基本通行码 72 及一由一特征抽取器 74 所抽取的输入资料的特征预设函数 73。除此，该基本通行码是一同步于该输入资料区块的随机变数产生器 70 所产生。结果，本实施例获得了实施例一及实施例二的益处。图 9 为编码及解码过程。很明显，甚至是输入被调整过的特征，该接收端 8 都不会还原出原来的编码金钥 86 来解密该资料。

实施例四：

本实施例与前一个相类似。但是，实施例四与实施例三不同之处在于，此时资料区块是被选取再抽取该特征。在本实施例，对应一资料区块的真实通行码是导自由其先前资料区块所取提的特征。该暂储存装置是用以留住最近的资料区块一个周期。其可于该特征抽取器留住该特征一周后被取代。于传输期间，只有该基本通行码递送至其他端，其可由一随机变数产生器所产生。该接收端是利用所接收的基本通行码，且执行相同的程序，以还原所需的编码金钥。图 10（A）及 10（B）

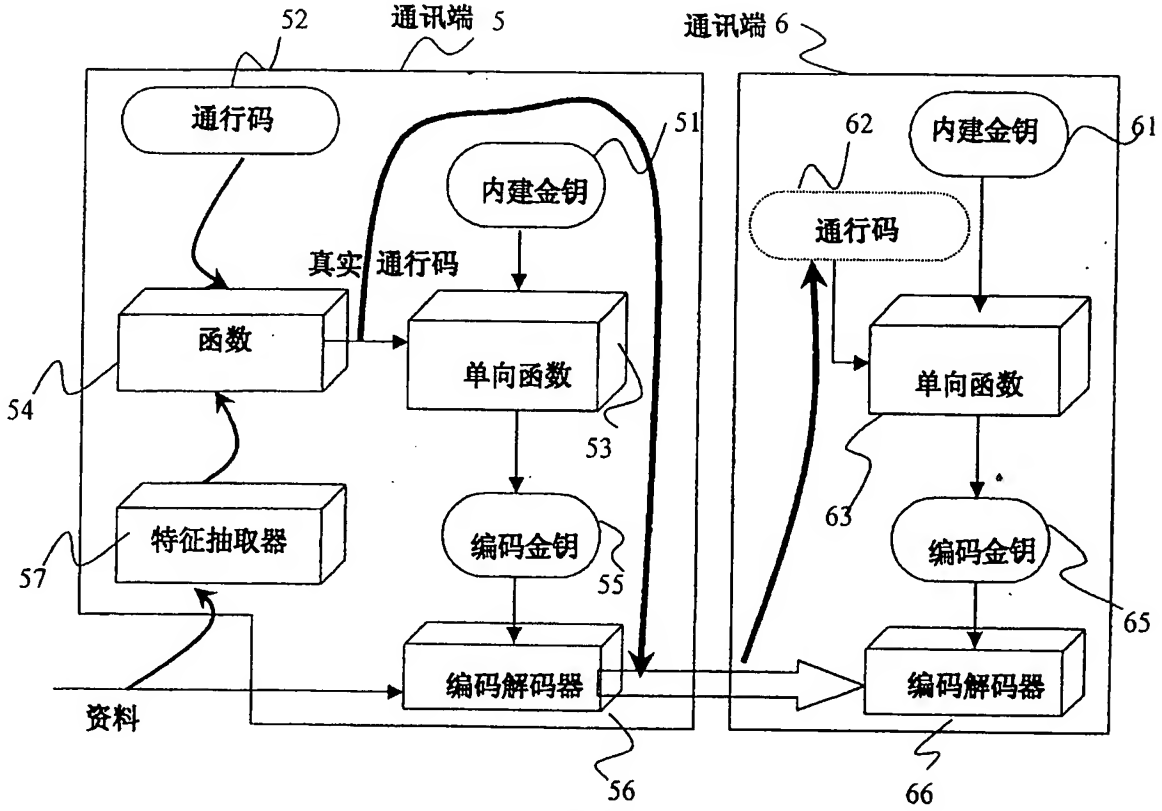

通讯端 5
通讯端 6
52
通行码
51
内建金钥
真实 通行码
函数
单向函数
54
53
特征抽取器
编码金钥
57
55
编码解码器
资料
56
62
内建金钥
61
通行码
单向函数
63
编码金钥
65
编码解码器
66

图 6

Method and system for tr. asmitting secret data of prot ting inside golden key and vairable pass code

Patent number: CN1304238

Publication date: 2001-07-18

Inventor: JIANCI HOU (VG)

Applicant: GUNETTYKEWAL INC BRITISH VIRGI (VG)

Classification:

- international: H04L9/00

- european:

Application number: CN19990126210 19991214

Priority number(s): CN19990126210 19991214

Abstract of **CN1304238**

The present invention relates to a transmission method of security information and is system. Said method includes the following steps: giving a first built-in gold key to its source terminal and a second built-in gold key to its target terminal; allocating said security information to complex number of information zone blocks and producing complex number of variable passing codes correspondending to one information zone blocks, and producing complex number of working gold keys, said working gold key is used for enciphering said information zone block, transferring said enciphered informationzone blocks and variable passing codes to said target terminal from source terminal, said variable passing codes received by said target terminal and the second built-in gold key are used for restoring said working gold key, and said restored working gold key is used for deciphering said enciphered information zone block.